THE FINANCIAL SERVICES COMMISSION

ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORISM

RISK ASSESSMENTS GUIDELINES

CONTENTS

ANTI-MONEY LAUNDERING AND PREVENTION OF TERRORISM
RISK ASSESSMENTS GUIDELINES

1.0 AUTHORITY

This Guideline is issued by the Turks and Caicos Islands Financial Services Commission (the Commission) under Section 43 of the Financial Services Commission Ordinance 2007 (the "FSCO") to assist financial businesses, for whom the Commission has regulatory and supervisory oversight, in complying with Regulation 17(1)(f) of the Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010 (as amended) (AML/PTF Regulations).

2.0 PURPOSE

2.1 This Guideline is intended for use by all financial businesses, as defined by Schedule 2 of the AML/PTF Regulations, in developing a business risk assessment that is –

- **instructive** in the development of each business' anti-money laundering and prevention of terrorist financing framework;
- **relevant** to the business; and
- **proportionate** to the risks faced by the business as determined by the nature, structure, and sector of the business, its customers and geographical location, the products and services offered and their delivery channels, and any other matter which may be relevant.

3.0 INTRODUCTION

3.1 The AML/PTF business risk assessment is a risk management tool developed by a financial business to set out its assessment of its likelihood or probability of being used for money laundering (ML) or terrorist financing (TF). This requires a comprehensive review of all the areas of the financial business.

3.2 Schedule 2 of the AML/PTF Regulations financial businesses include –

- **Regulated entities** namely: banks; trust companies; money services businesses; investment dealers/advisers; mutual funds; mutual fund administrators; company managers/agents; credit unions and long-term insurance business or any form of life insurance business or investment related insurance business that may be classified as general insurance business or a person who carries on business as an insurance intermediary where the person acts with respect to any type of insurance business referred to above.
- **Designated non-financial businesses and professions** for whom the Commission has supervisory authority, namely: accountancy and audit services,

realtors; legal professionals, consumer and mortgage lenders, high value dealers including jewellery stores and car dealerships; and

- **Non-Profit Organizations** for whom the Commissions has supervisory authority.

3.3 Throughout this guidance reference to "the business" means a financial business.

3.4 The risk assessment can serve as a valuable tool for any business wanting to manage its AML/PTF risks effectively. The key is to understand the risk exposure and develop the necessary policies, procedures, systems, and controls to mitigate the risk. Regulation 4 of the AML/PTF Code establishes the factors to be considered and documented by each financial business through a –

- **Business level risk assessment** which shall take account of all relevant risk factors including –

  i) the organisational structure, including the extent to which it outsources any of its activities;

  ii) its customers;

  iii) the jurisdictions to which its customers are connected;

  iv) the products and services offered;

  v) the nature, scale, and complexity of the activities of the financial business;

  vi) reliance on third parties for elements of the customer due diligence process;

  vii) new business practices and technological developments for new and existing products; and

  viii) any other relevant factors.

- **Customer risk assessments** using the same risk factors (above) to evaluate the risks linked to each client/customer relationship.

3.5 The risk assessment must be based on a documented consistent methodology that is understood by the parties who will use it and must be in a format that is acceptable to the Commission.

3.6 The risk assessment must be tailored to the nature, size, and complexity of the business. This means that a more detailed methodology is expected from a business that conducts complex or large volumes of transactions across various business lines or from businesses which have a higher risk for ML and TF.

3.7 The Risk assessments must be kept under regular and timely review and adjusted to reflect changing circumstances. Risks identified may change or evolve over time as triggered by new products, engaging new customers or geographies, new threats to the business, corporate changes, or occasioned by changes in the business' risk tolerance or regulatory changes.

3.8 A well-developed business risk assessment can be used to –

- identify gaps or opportunities for improvement in ML/TF policies, procedures, and processes; and
- assist management in ensuring that a risk-based approach is applied to the management of ML/TF risks, thereby enabling resources and priorities to be focused on those areas of higher risk.

Linking the business risk assessment to the customer risk assessment

3.9 One of the critical outputs of a portfolio analysis of ML/TF risks is the development of a consistent repeatable methodology for assessing ML/TF risks at the client level, using the prescribed risk factors to evaluate the level of risk that a client introduces to the business.

3.10 These evaluated risk factors are an analysis of the client's business activities, its clients and operating structure and should be considered when establishing an approach for risk rating individual client relationships. For example, if each of the risk categories are used to rate a client relationship, they can establish an overall money laundering risk score for the client. This score will allow that client to be ranked from a risk perspective relative to the client portfolio.

3.11 In assessing ML risk for tenured clients' relationships, focus must be given to the inherent risk characteristics presented by the client, which are described at 7.0 in this Guidance. The temptation to conflate longevity as a factor of the inherent risk should be ignored. Factors such as the longevity of client relationships is an output of effective control(s) such as the quality of due diligence undertaken, ongoing monitoring and interaction with clients over a period, which become a factor in determining the effectiveness of the controls and the residual risk.

3.12 A business should ensure that its internal controls are proportionately aligned to the risks posed by the range of its clients, where the highest risk clients will be the object of the most rigorous AML/PTF controls, whether through on-boarding standards, enhanced due diligence, enhanced monitoring and/or more frequent periodic reviews.

3.13 If a client or transaction is rated as having a high inherent money laundering risk, it does not mean it should be rejected. It simply means that enhanced controls to mitigate the higher level of money laundering risk need to be applied if the client is to be on-boarded and accepted, or the transaction performed. The additional controls to mitigate the higher

risk is referred to as enhanced due diligence (EDD). The EDD procedure should be documented and the application of EDD clearly demonstrable.

4.0 WHO IS RESPONSIBLE FOR THE RISK ASSESSMENT?

4.1 The board of a financial business has ultimate responsibility for undertaking the risk assessment. This enables the business to –

- **understand** how and to what extent it is vulnerable to ML/TF - its inherent risks.
- **measure** the exposure to ML/TF through an objective assessment of the mitigating controls around corporate governance, know your customer (KYC), customer due diligence (CDD), EDD, suspicious transaction reporting, training and record keeping; and
- **determine residual risk** by considering the inherent risk and the effectiveness of the mitigating controls in reducing/managing these risks.

4.2 The regulatory expectation is that the business will allocate appropriate resources and expertise to the development of the AML/PTF risk assessment. A risk assessment that is deficient in developing a clear understanding of the risk factors will not provide a sound basis upon which a robust and relevant AML/PTF risk management framework is to be implemented and maintained.

4.3 In assessing the operating environment, the adequacy and effectiveness of the resources and expertise required to manage the AML/PTF risk of the business must be considered. The board or persons responsible for governance and oversight, where the business operates as a non-corporate structure, are to ensure that AML/CFT responsibilities are clearly and appropriately apportioned.

5.0 FREQUENCY OF REVIEWS/UPDATES

5.1 The business should maintain an effective process for periodically reviewing and updating its risk assessment, ensuring that all changes are appropriately reflected. There are several reasons why a risk assessment should be updated. Foremost, is the requirement that the risk assessment reflects the business' current risk profile and to comply with regulatory standards.

5.2 Generally, risk assessments should be reviewed annually and where elements are considered to be high risk should be updated no longer than annually. Where the elements are considered to be medium risk, the assessment should be updated no longer that every two years and where risk elements are considered to be low the risk assessment should be updated no longer than every three years. Depending on the level of risk and resources available higher risk factors may be monitored more frequently than annually.

5.3 Ad hoc risk assessments may be performed to focus on higher risk areas or to address changes in risk factors and the specific controls that have been implemented to address the given risk. The results from the ad hoc assessments can be incorporated in the next scheduled risk assessment.

6.0 OVERARCHING ML/TF RISK FACTORS

6.1 Money laundering and terrorist financing risk can be defined as a function of three factors: threats, vulnerabilities, and impact. Threats and vulnerabilities put the business at risk of being used to facilitate ML/TF, and impact refers to the harm that ML or TF may cause.

6.2 Based on guidance issued by FATF[1], at the business level, a ML/TF risk assessment involves a systematic effort to identify threats and vulnerabilities and to evaluate the sources and methods of ML/TF and their impact on the business –

- **Threats** can be a person or people known to the business, which are internal or external to the business, or business activities with the potential to cause harm to the business or state. In the ML/TF context, a threat could include criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.

- **Vulnerabilities** refers to elements of a business that may be exploited by the identified threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focusing on the factors that represent weaknesses in AML/CFT systems or controls.

- **Impact** refers to the seriousness of the harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.

7.0 INHERENT RISK ASSESSMENT

7.1 Inherent risk represents the exposure to money laundering assessed before any consideration of mitigating controls. Each financial business must fully analyse the impact of each of the prescribed risk factors on the business (documented in paragraph 3.4), at both the business and customer levels.

7.2 How a business performs its risk assessment depends on several factors, including the size and scope of the businesses, its customer base, and its general risk assessment processes.

[1] The Financial Action Task Force (FATF) – the standard setting intergovernmental organization with responsibility for the design and promotion of policies and standards to combat financial crime.

As no two businesses are the same, inherent risk ratings may vary depending on the business or the business area that is being assessed.

The stages of a risk assessment

7.3 The risk assessment process can be divided into three stages: **identification, analysis, and evaluation**.

7.4 The three stages are described below:

- **Identification** starts by developing an initial list of potential risks or risk factors faced when combating ML/TF. These can typically be informed from known or suspected threats or vulnerabilities. Reports such as the National Risk Assessment and guidance issued by competent authorities and supranational bodies are helpful in the identification of potential threats. The identification process should be comprehensive; however, it should also be dynamic to enable new or previously undetected risks to be identified and considered at any stage in the process.

- **Analysis** is at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and impact of the identified risks or risk factors. ***The objective is to gain a holistic understanding of each of the risks, as a combination of threat, vulnerability, and impact, in order to assign a risk level or rank them in order of severity or importance.*** Each risk factor should be assigned a score which reflects the level of inherent risk associated with that risk and the prevalence of that risk compared to other risk factors.

- **Evaluation** involves taking the risks analysed during the previous stage and determining the priorities for addressing them. Prioritizing risk mitigation with limited resources requires a strategic approach. As a priority, address the risks that have the potential to cause the greatest harm to the business. Consider the effectiveness of the risk mitigating controls to determine the residual risk.

7.5 Once the inherent risks have been identified, considered, and documented, each risk must be assigned a risk level. **The overall risk assessment score is based on the collective ratings of the risks assessed.** The business should determine the approach to the risk scores by establishing a risk scale that is consistent with the size, type, and complexity of the business. Rating categories can be assigned as high, medium, and low or on a scale of 1 – 3 with three being the highest risk.

7.6 At the end of this process the business will be able to determine what is acceptable risk and what steps may be taken and by whom to limit any risks considered unacceptable.

7.7 Following the steps above, an assessment across the following risk categories must be undertaken:

Organizational structure

7.8 The inherent risk in the organizational structure considers whether the structure is complicated to the extent that supervision becomes onerous or conversely very simple and a supervisor becomes closely involved in routine operational activities.

7.9 Where the business is a sole practitioner, the typical "checks and balances" are not required to be undertaken. This situation may result in business acquisition objectives overriding the quality of AML controls, thereby increasing vulnerability.

7.10 The assessment would also consider risks related to a business' operating plan and any arrangements it has for the outsourcing of activities or where the business model heavily relies on third-party relationships.

Clients

7.11 The inherent money laundering risk of a business will vary depending upon differing client types. The following categories may be used as a guide to stratify the client base and to identify aspects of client risk:

a. *Ownership*: transparent or providing anonymity. For example, incorporation where there is no obvious rationale for the structure, and/or complex corporate structures.

b. *Politically Exposed Persons*: grouped because of the greater propensity for corruption.

c. *Industry types*: several industry types are recognised globally because of the increased likelihood of corruption. For example, the oil and gas sector, and the manufacturing or transporting of defence products sectors. Consideration of this grouping can apply both to corporate entities and individuals who may be owners or senior officials of companies operating within such sectors.

d. *Business activity*: for example, cash intensive businesses.

e. *Sources of income*: an individual with a regular salary, individuals who are self-employed.

7.12 It is important to recognise that client types will vary according to the business and the client portfolio. It is up to the business to stratify client types to demonstrate differing levels of ML risk. This process forms a solid and repeatable allocation of inherent ML risk presented by specific clients when undertaking the client level risk assessment. Care must be applied to those client types which may not be easily grouped. It is not unreasonable to have a group recorded as "other" but special attention should be made to those not easily grouped.

7.13 Each client type is assigned a risk score, depending upon the money laundering risk each type carries. This data can be utilized to determine what percentage of each business client types are rated according to the risk classification, e.g. low risk versus moderate versus high in order to determine the overall inherent client risk as a whole and by type. A business's approach to categorizing risk should be clearly documented.

Products and Services

7.14 The objective is to identify all products and services offered by the business and assess the inherent money laundering risk of each line of business. It is up to the business to consider all products and services offered and determine if there are variations in the level of money laundering risk. Businesses with many products and services (typically the banking sector) may consider limiting the focus to the top 5 to 10 most frequently used products and services and the propensity for money laundering to occur by use of the product or service.

7.15 In assessing products and services, it may be appropriate to consider the attractiveness to money laundering within the product, such as the availability of investment/placement features, levels of cash activity, availability of international money transfers, the degree of anonymity in the product. The materiality of the aforementioned factors within the portfolio of products and services must be considered.

Delivery Channels

7.16 The way in which a business communicates or interacts with its clients may affect money laundering risk. Differing delivery channels should be assessed as to whether, and to what extent, the method of account origination or account servicing, such as non-face-to-face account opening or the involvement of third parties, including intermediaries/introduces, could increase the inherent money laundering risk.

7.17 Cyber risks should be considered as part of the risk assessment. The information technology control framework should be sufficiently robust to help to ensure data integrity and mitigate data breaches.

Geography/country

7.18 Certain jurisdictions are more susceptible to money laundering and/or terrorist financing because of their potential to facilitate the movement, concealment and ultimately use of illicit funds.

7.19 Identifying geographic locations that may pose a higher risk is a core component of any inherent risk assessment and the business will seek to understand and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations.

7.20 The Geography/Country Risk may also be analysed with respect to the location of the business, and may also include its subsidiaries, affiliates, and offices, both internationally and domestically. The aim is to identify the geographic footprint of the client. For businesses, the aim is to identify the number of its clients with a connection to identified countries. The business will need to decide whether this number should be based on all or some of the following: domicile, incorporation, nationality, country of source of funds.

7.21 When conducting the assessment of country risk, consider whether the geographic locations in which the business or clients operate or undertake activities potentially pose a high risk for money laundering. Assess whether the countries to which clients transfer funds, and the countries from which the business receive funds could pose a high risk for money laundering activities.

7.22 There is no one single credible source for assessing country risk. However, sources of information are provided in Appendix D.

7.23 Any business which has a connection to a country or territory where any of the above considerations exist is presented with a higher risk of money laundering or financing of terrorism, and should have a high risk rating and be subject to increased scrutiny of transactions and dealings of the business.

Other risk factors

7.24 Several qualitative risk factors directly or indirectly affect inherent risk factors and can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in established key AML/PTF controls. For example, significant strategic and operational changes, such as the introduction of a major new product or service, a merger, or an acquisition, opening in a new location or closing an entity may affect the inherent risk. These changes may require a review of existing, or the establishment of new, internal controls, and given that these controls may take some time to become effective, the division, unit or business line will need to assess whether the inherent risk may have temporarily increased or changed.

7.25 Other qualitative risk factors might include:

Resources

7.26 Undertaking a risk assessment is considered a resource-intensive task. Conversely, an assessment undertaken without due care and attention to each step in the assessment process weakens the ability of the business to identify high risk activities and customer relationships. This leads to ineffective policies, procedures, and control systems. Such weaknesses undermine the risk assessment process and may result in regulatory censure.

7.27 The effective allocation of resources is key to the risk assessment. The level of detail to which a risk assessment can be developed is based on the information, data, and resources available. The information on which the risk assessment is based must be reliable.

Adequacy of information

7.28 The lack of information impacts the quality and completeness of the risk assessment. In instances where data cannot be easily sourced, in addition to identifying the information as "unavailable", the business must automatically assign a higher risk rating to the risk

factor until acceptable data is available for a proper analysis. Businesses are not given carte blanche on the issue of inadequate data, such matters are a subject of remediation.

Client base stability

7.29 The following matters may have an impact on the risk assessment:

i) Expected account/client growth

ii) Expected revenue growth

iii) Recent AML compliance employee turnover

iv) Recent/planned introductions of new products and/or services

v) Recent/planned acquisitions

vi) Recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs, offshoring)

Outcomes of the risk assessment

7.30 By completion of the inherent risk assessment exercise, the business should have:

i) A comprehensive list of risk indicators of money laundering activities that it reasonably faces;

ii) A quantification of the extent that the risk indicators are prevalent in its business;

iii) A money laundering inherent risk profile for the business; and

iv) An understanding of the process to manage changes in money laundering and terrorist financing risks.

8.0 RISK ASSESSMENT LINK TO THE COMPLIANCE PROGRAM

8.1 Many businesses fail to make the connection between the ML/TF risk assessment and the AML/PTF risk management control framework implemented by the business.

8.2 The identification and analyses of the ML/TF risks faced by a financial business is a key component in its risk management framework. The risk assessment identifies those areas posing the highest risk for money laundering, terrorist financing or other illegal activities. This information assists management in understanding the risk profile of the business as high, medium, or low; and indicates whether the risk mitigating controls are strong, moderate, or weak.

Risk Tolerance

8.3 Identification of the business' inherent risk reflects the reality of the business. As a best practice, it is timely to establish the business' risk tolerance. This is an important component of effective risk management and should be considered before moving to the

next step of considering how the identified risks can be addressed. When considering threats, the concept of risk tolerance will allow the business to determine the level of exposure (e.g. number of high-risk clients, inherently high-risk products, etc.) that is considered tolerable and can be accepted.

8.4 The business may want to consider the following risk categories which could be impacted:

- Regulatory risk
- Reputational risk
- Legal risk
- Financial risk

8.5 There is no legislation that prevents a business from having a high-risk tolerance. If the business is willing to deal with high-risk situations and/or clients, the Commission will expect that the mitigation measures or controls put in place (discussed in the following paragraph) will be commensurate and that residual risks are reasonable and acceptable.

8.6 In setting the risk tolerance, some helpful questions are:

- Is your business willing to accept regulatory, reputational, legal, or financial risks?
- What risks is your business willing to accept only after implementing some mitigation measures?
- What risks is your business not willing to accept?

9.0 INTERNAL CONTROLS

9.1 Internal controls are the policies, procedures and processes designed to limit and control risks and to achieve compliance with the law. The AML/PTF internal controls must consist of:

i) A risk assessment that is regularly reviewed and updated to reflect material changes in the risk factors and to identify those areas posing the highest risk for money laundering, terrorist financing and or illegal activities.

ii) A risk aligned AML/PTF Compliance Policies and Procedures Program with a system of controls to ensure compliance with regulatory requirements, to include amongst other things, the requirement for customer due diligence processes and ongoing monitoring, training and record keeping.

iii) A documented training plan that is tailored to the business and designed to ensure that on an ongoing basis employees are awareness of their legal obligation to make disclosures; that there is an understanding of the risk-based approach to prevention and detection of ML and TF, and that the plan is effective in monitoring the employees' ML/TF awareness.

iv) A Commission approved money laundering compliance officer responsible for oversight of the business' day to day compliance with policies and procedures.

v) A Commission approved money laundering reporting officer responsible for investigating suspicious activities and disclosures.

vi) Risk-based monitoring system to identify and report SARs.

vii) Periodic compliance reports to the board.

viii) Independent review and periodic testing of the compliance program undertaken by experienced compliance specialists to ensure effectiveness and adequacy of the program in relation to the risks faced by the business.

9.2 The compliance policy and procedures should incorporate, at a minimum, requirements for:

- customer due diligence measures and ongoing monitoring;
- reporting of suspicious activity and/or transactions;
- record keeping;
- employee screening; and
- risk assessment;

9.2 The policy and procedures should also address internal controls and –

- outline the process for the identification, detection and reporting of suspicious transactions;
- determine and explain what kind of monitoring is done for particular situations (i.e. low vs. high-risk clients/business relationships); and
- describe all aspects of monitoring: when it is done (frequency), how it is conducted, and how it is reviewed.

9.3 The extent to which an AML/PTF control is effective must consider the quality and capability of the people, processes and other resources employed in executing the control. For example, the risk that customer due diligence is inaccurate, incomplete, or not performed in a timely manner may be mitigated by a series of controls some of which are stronger than others.

9.4 The controls can be categorized as follows:

- *Preventative,* which prevents undesirable events and could include access controls, segregation of duties, and restriction on overrides or exceptions.
- *Directive,* which provides guidance to perform activities correctly and could include training, policies and procedures manuals, the use of form sets, aide-memoires, etc.
- *Detective,* which identifies that undesirable events have occurred, for example: exception reports and money laundering compliance officer or independent reviews.

9.5 A good control should be documented, repeatable, auditable, and provide a clear escalation process in the event of detected exceptions or breaches.

9.6 Control execution may be either manually performed or automated. It must be noted that the exception reports which provides alerts of out of character activity is regarded as semi-automated, as a person must review the alerts and make appropriate decisions.

9.7 Controls may be assessed as strong, moderate, or weak and the criteria for the assessments documented. An example of control assessment may be:

Strong	Policies and procedures aligned to legislative requirements. Control(s) evaluated, designed, and operating adequately, appropriately, and effectively.
Moderate	Policies and procedures were not always aligned to legislative requirements. A few specific control design and operating weaknesses, some of which are significant have been identified.
Weak	Numerous specific deficiencies in control design and performance, including the absence of alignment with legislative requirements. Controls evaluated are inadequate, inappropriate, or ineffective to manage the risks of money laundering.

10.0 CUSTOMER RISK ASSESSMENT

10.1 As part of the business risk assessment, Regulation 4 (1) (a) of the AML/PTF Code requires that the business assess the risks posed by its customers based on an analysis of customers/clients, using the same risk characteristics of client or customer types, products and services, delivery channels, geography and any other risk as may be relevant to the client relationship.

10.2 The customer risk assessment is relationship based. It considers details of the nature and purpose of the relationship identified from the customer due diligence information required from each customer. Documentation of the details of the business relationship helps in the monitoring of customer activity/transactions which can be compared to purpose and intended use of the account. The currency of information is relied on to determine the ML/TF risk through an understanding of the expected pattern of transaction activities of its customers.

10.3 Understanding the pattern and transaction activities of customers is helpful in the required monitoring of customers for changes in purpose and activity. It also ensures that where the ML/TF risks are impacted by the changes, that the risks are fully documented, and the risk level adjusted.

10.4 In applying the risk-based approach, the higher risk relationships would require greater risk mitigation measures, which includes more frequent assessments and greater involvement by management in determining corrective action. Such actions may include making a disclosure to the Financial Intelligence Agency (FIA) by filing a suspicious activity report (SAR) and possible termination of the business relationship. Lower risk relationships, while subject to ML/TF risk mitigating measures, could be assessed less frequently.

10.5 Certain products, services and delivery channels used by customers impact on the customer risk. Examples of higher risk considerations in the customer risk assessment are included in Appendix B.

11.0 EVALUATE RESIDUAL RISKS

11.1 As discussed earlier, the residual risk is the risk remaining after taking into consideration risk mitigation measures and controls. It is important to note that no matter how robust the risk mitigation and risk management program, the business will always have some exposure to residual ML/TF risks which must be managed.

11.2 Residual risk should be in line with the business' overall risk tolerance. The residual risk should not be more than the business is prepared to tolerate in the normal course of its operation. If it is identified that the residual risk is greater than the overall risk tolerance or that the measures and controls do not sufficiently mitigate the high risk situations or clients, the business should increase the level and/or quantity of mitigation measures in place.

11.3 The table below provides a methodology to determine residual risk taking into consideration the inherent risk factors and the assessment of controls. It encapsulates the processes described at paragraphs 7, 9 and 11 of this guidance and can be used at both the business and customer level risk assessments.

ASSESSMENT OF RESIDUAL RISK				
Inherent risk assessment		**LOW**	**MEDIUM**	**HIGH**
Assessment of Controls	**Strong**	Low	Low	Medium
	Moderate	Low	Medium	High
	Weak	Medium	High	High

Risk Response

11.4 Response to residual risk may be categorized in two broad types:

- Mitigated risks: Although they are "mitigated", they are still risks. These risks have been reduced but not eliminated. In practice, the controls put in place may fail from time to time (for example, the monitoring system or transaction review process fails, and some transactions are not reported).
- Tolerated risks: Although they are "tolerated", they are still risks. Acceptance means there is *no benefit in trying to reduce them*. However, the tolerated risks may increase over time, for example, when a new product is introduced, or a new threat appears.

12.0 EXPECTATIONS OF THE FINANCIAL SERVICES COMMISSION

12.1 The expectations of the Financial Services Commission are that:

i) As a best practice, the Board of Directors/Senior Management of the business will take the time to evaluate the level of residual risk.

ii) Businesses should confirm that the level of risk is aligned with what they are willing to tolerate to ensure the integrity of their own business. This approach is commonly referred to as risk appetite or risk tolerance.

iii) Upon completion of the risk assessment exercise, directors are urged to implement the risk-based approach as part of the day-to-day activities.

12.2 As referenced in paragraph 5.2, an important component of the risk assessment must include an annual review to test the effectiveness of the compliance regime. This includes at a minimum:

- The AML/PTF risk assessment
- Risk aligned policies and procedures
- Training program for employees and senior management.

12.3 If the business model changes, and new products and services are offered, the risk assessment must be updated along with the policies, systems, and controls.

12.4 The review of the assessment of ML/TF risk must cover all components of the compliance regime.

12.5 Businesses may choose to have their methodology reviewed regularly by an independent testing function, e.g. internal audit or an independent third party. This should allow for consistency of risk management with the business as well as provide a view of how the methodology compares across the industry.

APPENDIX A: CONSIDERATIONS FOR BUSINESS RISK ASSESSMENT

The table provides some examples of the type of factors to be considered in respect of the business risk assessment. It is not meant to be exhaustive and should be adapted to take account of the business' structure.

Business Structure – Elements that pose higher ML/TF risks

Risk Factors	Risk Considerations
○ Operational structure	Consider the operating structure, nature of the business, governance and oversight, management, industry, the number of branches, the number of employees and their functions, experience, and seniority as appropriate, and any concern for employee turnover.
○ Business model:	Consider the customer base, the method of delivery of product/service and whether customer interaction promotes customer anonymity.
○ Sector significance	Consider when the nature and economic importance of the business e.g. whether a bank, Money Services Business or a DNFBP. A business offering various products and services to a customer base of persons of mixed geographical locations will have different risks than a stand-alone business with a small customer portfolio whose customers and their activities are well known.
○ Training	The example above underscores the relationship between effective employee training programs, which are proportionate to the business risk, and are designed to ensure that all staff are able to identify higher risk factors and clearly understand their obligation under the AML/PTF legislation.
○ Outsourcing/third party service providers.	The financial business is ultimately responsible for its compliance regime. Where certain customer due diligence activities are outsourced to a third party, consider if there is (a) an understanding of the operations of the third party and (b) an effective oversight regime of the services provided.
○ Groups/affiliates	Consider the extent to which any risk resulting from groups/entities activities (internal or external) impacts the business. This could arise in situations where the business is part of a group or is affiliated with other businesses through common ownership, directorship, and customers.
Multi-layered Structures	Transparency in beneficial ownership is a legal requirement; hence, there must be consideration for the extent to which opacity in the business' ownership obscures the identity of the true beneficial owners.
○ Relationship with multinational Institutions	Consider the risks related to a parent or shareholding relationship where the parent/shareholder, based outside of the jurisdiction, sets group-wide policies that may not adequately reflect local legislative requirements.
○ International Correspondent Banking.	Consider the possibility that there could be a situation where a traditional correspondent banking account is established, and the local branch is not aware that the foreign financial institution is allowing customers to conduct anonymous transactions through the TCI bank account.

Customers

Risk Factors	Risk Considerations
○ Ownership structure	Consider factors such as whether the customer is a corporate entity or otherwise, and whether domestic or international.
○ Industry	Consider whether there is sufficient understanding of the risks related to the industry with which the customer is associated.
○ Politically Exposed Persons (PEPs)	The law identifies PEPs as high risk. Consider how this factor has been addressed by the business in the risk assessment.
○ Connection to high-risk countries:	Certain countries are identified as posing a high risk for ML/TF based on factors such as their level of corruption, the prevalence of crime in their region, the weaknesses of their money laundering and terrorist financing regime, and identified by FATF as non-cooperative.

Geography – higher risk considerations

Risk Factors	Risk Considerations
○ Location of business	Consider the risks posed by TCI's geographic location - for example, risks posed by factors such as TCI's porous borders and its implications. Consider the countries with which the business' principals are connected or carry on business and the risks associated with those factors.
○ Events and matters of public interest	Domestic and international events could impact a business. Consider how matters of public interest, which affect the jurisdictions with which the principals of the business are connected, may have legal, reputational and/or regulatory implications which pose higher risk.
○ Connection to high-risk countries:	Certain countries are identified as posing a high risk for ML/TF based on factors such as their level of corruption, the prevalence of crime in their region, the weaknesses of their money laundering and terrorist financing regime, and identified by FATF as non-cooperative.
○ Sanctioned countries: ○ UN Security Council Resolutions. ○ EU Sanctions ○ Financial Action Task Force (FATF) List of High-Risk Countries and ○ Non-Cooperative Jurisdictions. EU Sanctions List	**Sanctions** may apply to dealings with countries, terrorist organizations or designated persons from a target country and can impact a financial business by – • Prohibiting trade and other economic activity with a foreign market; • Restricting financial transactions; or • Leading to seizure of property in both the domestic and other jurisdictions. The extent to which a business is impacted by international sanctions must be considered – Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions-0 Consolidated list of persons, groups, and entities subject to EU financial sanctions. https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions High Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

Products and Services which may pose a higher risk of ML/TF

Products: ○ Bank drafts. ○ Products offered through intermediaries/agents.	Legitimate products and services can be used to mask the origins of illegal funds to hide the identity of the owner or beneficiary of the products or services. Consideration should therefore be given to the market in which the financial business operates and to whom the products or services are directed. The type of business or individuals to whom the products and services are directed determines the impact of these risk factors.
Services: ○ Electronic funds transfers ○ Electronic cash ○ Letters of credit ○ Private banking ○ Shareholding services	Certain products and services lend themselves more easily to abuse by customers and third parties; therefore, this element of risk must be considered.

Delivery Channels which may pose higher risks

Risk Factors	Risk Considerations
○ Non face to-face transactions	The ML/TF risks are inherently higher where services offered use non face -to-face transactions, agents or where applications can be made on-line. The anonymous nature of non-face-to-face transactions and services, for example virtual currency and certain referred customer relationships, may have inherently higher risks for ML/TF.
○ Agent	The law makes the financial business liable for any failures to apply due diligence measures; therefore, consideration should be given to the use of agents whose activities may not be subject to the AML/PTF standards.

New business practices and/or technological developments

New Technologies ○ Quick anonymous payments	Financial businesses must consider the products or services that are based on new technologies and their impact on the inherent risks to the business. Examples of payment methods used to transmit funds more quickly or anonymously include e-wallets, pre-paid cards, internet payment services, digital currency, or mobile payments.

Other factors with ML/TF relevance

(International standards, regulatory guidance, and potential threats)

Regulatory Guidance	The risk assessment should consider guidance issued by TCI's competent authority as well as that issued by supranational organizations from time to time. www.tcifsc.tc
National Risk Assessment	The National Risk Assessment carried out on the TCI considered the inherent risks of ML/TF across sectors, products, and customers. This included an assessment of government, public authorities, law enforcement agencies and financial institutions and may be helpful in identifying the AML/PTF risks in the supervised sectors. https://tcifsc.tc/wp-content/uploads/2019/02/national-risk-assessment-report.pdf
FATF's AML/PTF risk assessment of the TCI	The FATF assessment of the implementation of AML/CFT measures in the TCI was documented in a Mutual Evaluation Report. https://www.fatf-gafi.org/countries/s-t/turksandcaicosislands/documents/mutualevaluationoftheturksandcaicosislands.html As the international standard setter, FATF has issued guidance on AML/CFT risks posed by activities in the various sectors to include – Guidance on Risk-Based approach for the Banking Sector http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-trust-company-service-providers.html FATF Guidance on the Risk-Based Approach for Money Services Businesses https://www.fatf-gafi.org/documents/documents/fatfguidanceontherisk-basedapproachformoneyservicesbusinesses.html FATF Guidance on the Risk-based Approach for the Life Insurance Sector http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf FATF Guidance on the Risk-based Approach for the Securities Sector https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/rba-securities-sector.html?hf=10&b=0&s=desc(fatf_releasedate) Guidance for a Risk-Based Approach Guidance for Legal Professionals https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-legal-professionals.html

Trends, typologies and Threats of ML/TF:	FATF Guidance for a Risk-Based Approach for the Accounting Profession https://www.fatf-gafi.org/documents/riskbasedapproach/documents/rba-accounting-profession.html?hf=10&b=0&s=desc(fatf_releasedate) FATF Guidance on the Risk-Based Approach for Real Estate Agents https://www.fatf-gafi.org/documents/documents/fatfguidanceontherisk-basedapproachforrealestateagents.html FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones https://www.fatf-gafi.org/documents/documents/fatfguidanceontherisk-basedapproachfordealersinpreciousmetalsandstones.html Trends and typologies have been developed by FATF on ML/TF methods used in specific sectors and who the main ML/TF actors are – http://www.fatf-gafi.org/publications/methodsandtrends/?hf=10&b=0&s=desc(fatf_releasedate)

APPENDIX B: HIGH-RISK CUSTOMER RELATIONSHIP CONSIDERATIONS

The table lists examples of high-risk indicators on certain products, services and delivery channels used by the customers/clients their impact on the client risk assessment.

Product risk

Products will have a higher inherent risk where there is **customer anonymity,** where the **source of funds/source of wealth** information has not been provided, and where **customer due diligence is incomplete.**

High risk indicators	Impact/ rationale
Clients using **electronic funds payment services:** o Electronic funds transfers o Stored value cards (electronic cash) e.g. prepaid cards	**Electronic funds transfers** can be conducted as non face-to-face and large amounts of money can be transmitted and can disguise the origin of the funds. **Electronic cash** is a high-risk service because it can allow parties to conduct transactions without being identified.
Clients use products such as: o bank drafts and o letters of credit	**Bank drafts** can move large amounts of funds without the bulkiness of cash. These products are similar to cash as the holder of a draft could be considered the owner of the money, e.g. a draft payable to a financial institution; as such, the draft could be passed on to another person thereby blurring the trail of the money. This risk is mitigated if the draft is issued payable to a specific payee. **Letters of credit** are a guarantee from a bank and a seller will receive payment for goods. Letters of credit have a higher inherent risk for ML/TF as they can be used in trade-based transactions to increase the appearance of legitimacy and reduce the risk of detection.
Clients use non face-to-face products and services offered through intermediary agents and introducers	**Non face-to-face transactions** make it more difficult to ascertain the identify of clients. **The use of intermediaries or agents** may increase a business' risk as they may not be subject to ML/TF laws and/ measures may not be adequately supervised. As considered under the business risk assessment, the law makes the business liable for any failures to apply due diligence measures; therefore, consideration should be given to the use of agents whose activities may not be subject to the AML/PTF standards. The business should have a system of ensuring the appropriate level of customer due diligence procedures (which include background checks and ongoing monitoring) are in place to reduce the risk of this type of relationship being used for ML/TF through its agent network.

Geography

In the customer risk assessment, the geographic footprint of the client or business relationship and its impact on the business is considered. A business faces increased ML/TF risks when funds are received from or are directed to high risk jurisdictions, and when a client is connected to a high-risk country. Risks such as residency, citizenship or transactions should be assessed as part of the inherent risks associated with clients.

High risk indicators	Impact/ rationale
Client's proximity to a branch	A client that conducts business or transactions away from their home branch without reasonable explanation should be noticed. Example: • A client owning a single-location business makes deposits on the same day at different branches in the geographical area that does not appear to be practical.
Non-resident clients	Identification of these clients may prove more difficult as they may not be present, and this should raise the inherent level of risk.
Clients conducting Offshore business activities.	Has a legitimate reason been provided for this? In the absence of a plausible explanation it could be perceived that the offshore activities may be used to add a layer of complexity to transactions and relationships and this should raise the overall risk of ML/TF.
Client's connection to high-risk countries.	The client's connection to high-risk countries should be considered as some countries have weaker or inadequate AML/PTF standards, insufficient regulatory supervision, or simply present a greater risk for crime, corruption, or terrorist financing.

Service Risks

Service risks are higher in instances where the customer is using a service that the law or international standard identifies as higher risk for ML/TF. For example, electronic funds transfers, international private banking services, international correspondent banking services, company shareholding and directorship services.

Delivery Channel Risks

Delivery channel refers to the method that is used to obtain a product or service or through which transactions can be conducted. While many channels do not bring the client in direct contact with the business, non face-to-face customer interaction has the potential to obscure the true identify of a client or beneficial owner which poses higher risks. This is the case with internet banking, debit cards transactions, account origination servicing. Such services used alone or as part of a combination of services to customers are considered high risk.

Client characteristics and patterns of activity

High Risk Indicators	Impact/rationale
Client holding property believed to be controlled by or on behalf of a terrorist group.	The business is required to make disclosure to the FIA if it is believed that a customer owns or controls property on behalf of a terrorist group. This includes information about transactions or proposed transactions relating to that property. Once the Suspicious Transaction Report is filed, the client automatically becomes high-risk.
Client is a Politically Exposed Person (PEP)	The law considers PEPs high risk. A PEP is an individual who is or has been entrusted with a prominent public function. The position they hold may make them vulnerable to ML/TF or other offences such as corruption. A business must consider a politically exposed person high risk.
A customer that has complex structure that conceals the identity of the beneficial owners	The AML/PTF Regulations require that the business obtains information on the identity of beneficial owners of the customer. This applies to an individual who is an ultimate beneficial owner of the legal person, partnership, or arrangement. If the business is unable to complete the verification of the identity of the beneficial owner, the business shall terminate the business relationship with the customer.

Other high-risk indicators and rationale

High-risk indicators	Rationale
A SAR previously filed or considered	Suspicious activity and/or transactions or attempted transactions are financial transactions that a business has reasonable grounds to suspect are related to the commission of a ML/TF offence. Filed SARs/STRs should elevate the risk of the client or business relationship.
Transactions involving third parties	Suspicion arises when transactions involve third parties. For securities dealers, suspicion in relation to third parties may relate to the source of funds deposited to securities accounts or to the use of funds following withdrawals from securities accounts. Such transactions within the activity sector could be indicative of the layering stage of money laundering activity.
Account activity that does not match client profile	Customer account activity that does not match the client profile may indicate a higher risk of ML/TF. The business may have a customer (who is unemployed or a student) made several large cash deposits which does not match the profile of the customer.
Client's business generates cash for transactions that are not considered cash intensive	The business has no legitimate reason to generate cash and this represents a higher risk of ML/TF.
Client's business is cash intensive (bars and clubs)	Cash intensive businesses may have a higher inherent risk for ML/TF.
Clients offering on-line gambling	FATF has indicated that internet payments are an emerging risk in the gambling industry. Internet payment systems are used to conduct transactions related to online gambling, these two factors making the online gambling industry inherently high-risk. Higher internet risk may exist in the online gambling activities if not effectively supervised.
Client's use of unusually complex structure	Unnecessarily complex structures or complexity in customer transactions may indicate that the client is trying to hide transactions and/or suspicious activities. Example for securities dealer: • Frequent contributions and withdrawals from securities accounts,

	• Transfers between accounts for no particular reason.
Client is a financial institution with which the business has a correspondent banking relationship and/or Client is a correspondent bank that has been subject to sanctions	Some countries have weaker or inadequate anti-money laundering and anti-terrorist financing standards, insufficient regulatory supervision, or a greater risk for crime, corruption, or terrorist financing. The nature of the businesses that a correspondent bank client engages in, as well as the type of markets it services, may present greater risks. That a client has been subject to sanctions should raise the risk level and appropriate measures should be put in place to monitor the account.
Client is a DNFBP (lawyer or accountant) holding accounts for others unknown to the business	Accountants and lawyers sometimes hold co-mingled funds where the beneficial ownership may be difficult to verify. This is not to suggest that all clients with these occupations are high-risk. However, the business must understand that risk exists for these occupations and it will be up to the business to determine if the activities and/characteristics of these clients are in line with their expectation.
Client is an unregistered charity	Charities may be misused by individuals or other organizations to assist in money laundering schemes or finance/support terrorist activity. It is important to be aware of the risks in relation to charities and to apply due diligence by confirming that the charity is registered with the NPO Supervisor.

APPENDIX C: CONSIDERATIONS WHEN ASSESSING CONTROL DESIGN EFFECTIVENESS.

Questions for Assessing Design Effectiveness	Points to Consider	Control assessment (Strong, Moderate Weak)
Does the Control address the relevant risk, designed effectively, and proportionate to the risk	○ Each control should have a control objective. ○ Assess the strength of control by its class i.e. Directive preventative, detective, ○ is the control manual, semiautomated, or automated?	
If the risk is in the context of a process, does the control cover all the relevant types of transaction.	○ Does the control cover all transaction types adequately? ○ Have any new transaction types come into scope that need to be addressed?	
Is the control being applied on a sufficiently frequent basis.	○ If the control was to be applied on a more frequent basis, would there be a proportionate reduction of risk? ○ If errors are found due to the application of the control, are they being resolved in a timely manner?	
Does the detail of the control still address all in-scope aspects of the risk?	○ If the underlying process has changed, has the control been appropriately changed e.g. with a checklist are the checkpoints still valid and complete.?	
Does the person performing the control have sufficient skills or experience to operate the control.?	○ Length of experience of in operating the control. ○ Relevant previous experience, qualifications, and training. ○ Nature and complexity of the control as compared to the level of the individual in the business. ○ The ability of the control operator to articulate the risk and what the control is trying to achieve and control, as well as their understanding of the said risk especially where judgement is used in the performance of a control.	
Is evidence of the operation of the control appropriately recorded and capable of being tested.	○ If a control requires the operator to follow steps on a checklist, does the design of the control require that the steps on the checklist are supported with adequate evidence? Is the level of detail required adequate? ○ Would the control operate more effectively with the use of Key Indicators to monitor control performance? ○ Is the level of analysis and evidence of review expected sufficient (including the appropriate level of management involvement) particularly based upon the level of risk involved?	
Have issues ever arisen due to the failure of this control? If so, what is the frequency of those issues?	○ How recent were the issues? ○ What were the root causes of failures and have they been addressed E.g. operator error addressed through training?	
Is the control design properly documented?	○ Are the objectives of the control clear? ○ Are the steps / process that need to be followed clearly documented and east to follow? ○ If appropriate is there a checklist to aid operation?	

APPENDIX D: SOURCES OF INFORMATION FOR ASSESSING COUNTRY RISK

1. The Financial Action Task Force provides commentary on the following
   a. High Risk and other monitored countries.
   b. Improving Global AML/CFT Compliance, an ongoing process.
   c. Outcomes of the mutual evaluation process, referred to as Consolidated Assessment Ratings.

   http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-february-2019.html
   http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-february-2019.html
   http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)

2. International Narcotics Control Strategy Report
   Prepared annually by The US State Department; provides reports on many countries.
   https://www.state.gov/2019-international-narcotics-control-strategy-report/

3. The Financial Crimes Enforcement Network (FINCEN) a bureau of the United States Department of the Treasury that collects and analyses information about financial transactions to combat domestic and international money laundering, terrorist financing, and other financial crimes.

   It is important to consider country risk within countries. The FINCEN website provides information in respect of the United States

   - High Intensity Drug Trafficking Areas (HIDTA)
     https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a009
   - High Intensity Financial Crime Areas. (HIFCA)
     https://www.fincen.gov/hifca

4. There are also two useful, subscription services for assessing country exposure.
   - Basel AML index
     https://www.baselgovernance.org/asset-recovery/basel-aml-index
   - Know Your Country
     https://www.knowyourcountry.com/country-ratings-table